New Trends in Psychology

Thinking Patterns in Decision-Making in Information Systems

Florentina-Loredana Dragomir[1]

Abstract: The paper brings to the forefront the patterns of thinking used in national security information systems. The predictive models that underlie decision-making are presented and the psychological and technological vulnerabilities of cognitive biases are specified, as well as solutions for their correction. The improvement of national security by optimizing information systems with machine learning-based algorithms is emphasized.

Keywords: information systems; predictive models; psychological models; machine learning; national security

1. Introduction

The intersection of psychology and information systems offers valuable opportunities for developing technologies that not only improve the efficiency and effectiveness of processes but also respect and promote the well-being of users. By deeply understanding human behavior and applying this knowledge to the design and implementation of information systems, we can create technological solutions that are both powerful and ethical. Psychology and information systems, while

[1] Associate PhD, Faculty of Security and Defence, National Defence University Carol I, Bucharest, Romania, Address: 68-72 Panduri St., sector 5, 050662, Bucharest, Romania, Corresponding author: florentinaloredana.dragomir@gmail.com.

seemingly distinct fields have many intersections that can lead to the development of more effective technologies that are tailored to human needs. Psychology focuses on understanding behavior and mental processes, while information systems deal with the collection, processing, and use of information, often through technology. Integrating these two fields can improve human-machine interaction, optimize decision-making processes, and address ethical challenges associated with the use of artificial intelligence (AI).

In a turbulent geopolitical context, tormented by political-military transformations, in which security information is vital for the protection of the state, understanding the way people and algorithms make decisions becomes crucial, knowledge patterns thinking used in systems informational, model-based psychological, and cognitive that influence security nation by their impact can be minimized manipulation in information warfare. The model's psychological factors that determine the process of decision-making, analysis dates, and defense strategies in cybernetics are directions key for predictive models of making security decisions.

2. Psychological Models in Decision Making

The psychological study of the process has provided the development of several models that explain how individuals make decisions in various contexts. The fundamental reference model is *the Rational Model* (Brown & Green, 2022), which suggests that individuals follow a series of logical steps to make optimal decisions. These steps include identifying the problem, gathering relevant information, generating options, evaluating them, and choosing the best solution. This model assumes that decision-makers have access to all necessary information and can process this information without cognitive limitations. However, in practice, people often face cognitive and informational limitations, which led to the development of *the Bounded Rationality Model* (Simion, 1995). This model, proposed by Herbert Simon, recognizes that individuals cannot analyze all possible options due to time and resource constraints. Instead, they use heuristics and make satisfactory, rather than optimal, decisions. Another approach has generated an equally important model developed by Daniel Kahneman and Amos Tversky, namely Prospect Theory. This theory suggests that people evaluate gains and losses differently, tending to be more sensitive to losses than to equivalent gains. Thus, decisions are influenced by the way options are presented or framed, a phenomenon known as "framing" (Kahneman & Tversky, 1979). The Intuitive-Decision Model (Smith & Doe, 2021)proposes that many decisions are made quickly, based on intuition and previous experience, without deliberate analysis. This model is relevant in situations where decisions must be made quickly or under conditions of uncertainty. In contrast, the Recognition-First Model (Klein, 1993) suggests that experts recognize familiar patterns in complex situations and choose an action based on this recognition, quickly assessing whether it will work or not. This model is frequently observed in fields such as medicine or aviation, where experience plays a crucial role in decision-making. The *Career Decision-Making Process Model* (Harren, 1979), proposed by Harren, identifies three decision-making styles: rational, intuitive, and dependent. The rational style involves a logical and systematic analysis of options, the intuitive style relies on feelings and impressions, and the dependent style involves seeking advice and approval from others. *Expected Utility Theory* (Evans, 2022) suggests that individuals make decisions by evaluating the anticipated utility of each option and choosing the one that maximizes this utility. This theory assumes that people are rational agents who make decisions to maximize their benefits. *The Heuristics and Bias Model* (Gigerenzer & Gaissmaier, 2011) emphasizes that people use simple rules, called heuristics, to make complex decisions. While these heuristics can be useful, they can also lead to systematic errors or biases. For example, the availability heuristic involves assessing the probability of an event based on the ease with which examples come to mind, which can lead to overestimation of the frequency of dramatic events. *The Group Decision Making Process Model* (Garcia-Retamero & Dhami, 2020) analyzes decision-making dynamics in group contexts, highlighting phenomena such as groupthink, where the desire for consensus can lead to suboptimal decisions, and group polarization, where group discussions can lead to the adoption of more extreme positions. The understanding of how individuals make decisions has been deepened in recent literature, with an emphasis on various psychological models. A notable model is *the Intuitive Decision Theory*, which emphasizes the role of intuition and experience in making quick decisions, especially in situations of uncertainty. The model suggests that decision makers rely on pattern recognition and intuitive judgments to make effective decisions. Human emotions have also influenced human decision-making, and another model, *the Emotion-Based Decision Theory* [8], explores how they disrupt the decision-making process. Studies show that emotions can serve as valuable signals in evaluating options and can guide decision-making behaviors, influencing the perception of risk and reward. *The Adaptive Rational Decision Model* also proposes that individuals adjust their decision-making strategies according to the complexity of the task and the cognitive resources available. In this situation, the model suggests that decision-makers may oscillate between analytical and intuitive approaches, depending on the demands of the situation. In addition, *Social Decision Theory* examines the influence of social factors on the decision-making process. According to this theory, social norms, expectations, and group dynamics can shape individuals' choices, sometimes leading to conformity or polarized decisions. They provide valuable insights into the complexity of human decision-making, highlighting the interplay between cognitive, emotional, and social factors. The variety of psychological models of decision-making provide diverse perspectives on the act itself, emphasizing the complexity and multidimensionality of how people make decisions.

3. Predictive Models and Decision-Making in National Security

Predictive psychological models play a key role in understanding and anticipating human behavior, and this capability becomes extremely valuable in the context of information warfare, especially in an international political climate marked by tensions and strategic competition. When advanced algorithms, big data analysis, and artificial intelligence are used to identify patterns of thought, emotions, and reactions to external stimuli, it allows state and non-state actors to influence collective decisions and perceptions in an extremely precise way.

We can say with certainty that in information warfare, where narrative manipulation and perception control are essential, predictive models are used to analyze the psychological vulnerabilities of target groups. After analyzing the predisposition to disinformation, the level of social polarization or the tendency towards radicalization, a better targeted and effective propaganda can be woven. For example, by analyzing discourses on social networks and digital interactions, it is possible to predict how certain segments of the population will react to specific messages and how their impact can be amplified through micro-targeting techniques. States that have advanced capabilities in the field of artificial intelligence and data analysis can optimize their influence strategies, exploiting the psychological weaknesses of their opponents and strengthening their own position. Thus, information warfare is no longer just a simple fight for narrative control, but becomes a sophisticated confrontation, based on psychometrics, neuroscience and predictive behavior. In this context, a vicious circle is created in which states and non-state actors must constantly improve their defense and counter-manipulation capabilities. If in the past propaganda was generalized and disseminated through traditional channels, today it is highly personalized, adapted to the psychological profile of each individual or community, transforming information warfare into a form of social engineering on a global scale. National security decisions are significantly influenced by human cognitive biases, and the use of predictive models and advanced artificial intelligence algorithms seeks to mitigate these effects. Threat analysis systems use supervised machine learning algorithms, which rely on historical data sets to identify patterns, but can inherit and amplify developer biases. In this process, decision-making models based on artificial neural networks are used to detect anomalies in data traffic, but can provide distorted results when the training data is incomplete or biased. In the field of disinformation, natural language processing algorithms are essential for identifying manipulation campaigns, but can be vulnerable to sophisticated tactics that exploit resonance chambers and the framing effect. Classification systems used in social networks operate through deep learning models, adjusting the flow of information according to user interactions, which can amplify polarization and reinforce existing cognitive biases. In cyber defense, intrusion detection algorithms based on unsupervised learning analyze abnormal behaviors, but can generate false alarms due to the tendency to anchor models in historical data. In crisis situations, the use of automated decision systems through evolutionary algorithms can optimize the response to attacks, but the lack of human interpretation can lead to wrong decisions in the face of unforeseen threats. Thus, the balance between human analysis and the use of advanced algorithms remains essential in strategic decision-making, in a security landscape where threats are constantly evolving and psychological and technological vulnerabilities are actively exploited. In an information system based on cognitive biases and heuristics, the psychological model can be integrated into the decision processing and analysis component, where data is interpreted and recommendations are generated for users. This component uses artificial intelligence algorithms and cognitive modeling techniques to understand and predict user behavior based on cognitive biases and heuristics.

4. Vulnerabilities in Implementing Psychological Decision-Making Models

The decision processing and analysis component works by applying advanced psychological models, using algorithms such as Random Forest, neural networks and Bayesian analysis to interpret data and predict user behaviors. It receives information from the data collection component, where various sources, such as interaction history, sensors, and external databases, provide the necessary input to train predictive models. Supervised machine learning systems are used to analyze behavioral patterns and adapt recommendations based on identified cognitive biases, such as confirmation bias or anchoring. The collected information is managed by the data storage and management component, where Big Data technologies allow the efficient organization of large volumes of information required for behavioral analysis. The decision models are subsequently applied in the main processing component, where neural networks detect complex relationships between variables, and bayesian analysis adjusts predictions based on new data received. In the final interaction with the user, the interface and feedback component optimize the display of information, using personalization algorithms to influence decisions subtly and effectively. Machine learning-based recommendation models adapt the options presented based on past behavior, while behavioral data analysis adjusts the dynamics of the interaction to improve the user experience. Thus, the entire system functions as an integrated decision-making mechanism, where advanced information processing algorithms allow for continuous adaptation to the real way users react to stimuli and make choices. Improving national security by optimizing information systems requires the integration of advanced algorithms that reduce the impact of cognitive biases in the decision-making process. Hybrid decision-making systems combine human analysis with explainable artificial intelligence models, such as bayesian networks and Random Forest algorithms, allowing for the validation of automated decisions and the prevention of strategic errors. Explainable AI plays a key role in this approach, providing transparency in data interpretation and justifying decisions made through more understandable models, unlike deep neural networks, which function as “black boxes”. Correcting cognitive biases in data analysis involves the use of decision-making pattern detection algorithms, capable of identifying erroneous trends, such as confirmation bias or anchoring. Counterfactual models based on supervised machine learning are used to generate decision-making alternatives, forcing analysts to consider different scenarios. In this sense, natural language processing algorithms and advanced linguistic analysis are essential in detecting disinformation, evaluating sources and verifying the authenticity of information propagated on social networks. Convolutional neural networks are used to identify subtle patterns of media manipulation, while unsupervised clustering algorithms can detect coordinated disinformation campaigns. Cybersecurity benefits from adaptive AI, capable of recognizing new attack patterns through reinforcement learning techniques, in which models are trained to adjust their strategies based on emerging threats. Augmented reality-based simulations and alternative scenarios are used to train decision-makers, allowing testing of reactions in crisis situations through multi-scenario simulators supported by advanced predictive models. By implementing double-validation mechanisms and multidisciplinary teams that independently analyze the same data, the effects of attribution bias and overreliance on single sources are reduced. Automated decisions in national security are monitored by AI audit mechanisms, which use interpretability algorithms, such as LIME (Local Interpretable Model-Agnostic Explanations), to explain the reasons behind certain classifications. Control of AI decisions is strengthened by introducing human intervention protocols, where analysts can evaluate and correct the results generated by predictive models. In this way, information systems become more robust, able to cope with emerging threats without falling prey to errors induced by cognitive biases, ensuring effective protection of national security.

4.1. Ethics and Transparency in National Security Decision-Making Systems

The use of artificial intelligence (AI) and information systems in the field of national security has become a necessity in the face of increasingly complex and diverse threats. However, this technological integration raises significant ethical issues that cannot be ignored. Questions of algorithmic transparency, surveillance and respect for citizens' rights are at the heart of the debate on how technology should serve security interests without compromising fundamental democratic values. One of the main ethical challenges is the lack of transparency of the algorithms used in threat assessment. Machine learning models, especially deep learning, are often considered "black boxes" due to their complexity and the difficulty of explaining their internal decisions. In the context of national security, where the stakes of decisions are extremely high, the lack of clear justification for the measures taken can lead to arbitrary decisions or abuses of power. For example, an automated suspect identification system based on facial recognition may have systematic errors, leading to the wrong profiling of groups of people and violating the principles of fairness and justice. Excessive surveillance is another major problem, especially when technology allows for the large-scale monitoring of the population. In the desire to prevent terrorist attacks or subversive activities, security agencies may implement surveillance systems that conflict with the fundamental rights of citizens, such as the right to privacy. In a democratic state, this fine line between collective protection and individual freedoms must be managed very carefully. Trust in state institutions can be seriously damaged if citizens perceive that they are constantly being watched or that they are being treated as suspects until proven otherwise.

To maintain the balance between security and freedom, it is essential to develop clear policies to guide the use of AI for security purposes. These policies must include democratic accountability mechanisms that ensure that algorithmic decisions are subject to independent scrutiny and evaluation. In this regard, adopting the principles of Explainable AI can contribute to increasing transparency by providing understandable explanations for the decisions taken. In addition, the involvement of ethics committees in overseeing the application of AI in national security can ensure that democratic values are respected and the risks of abuse are minimized.

In conclusion, the ethical challenges associated with the use of AI in national security should not be underestimated. While the technology can bring undeniable benefits in preventing and managing threats, its implementation must be accompanied by a strong commitment to transparency, respect for citizens' rights, and democratic accountability. Only in this way can we ensure that security measures do not undermine the very principles they are supposed to protect.

5. Conclusion

Patterns of thinking used in systems information influence security nation by their impact on process decision-making, defense cyber, and management misinformation. Understanding cognitive biases and their correct integration into AI systems can lead to decisions that may be advised and to a security nation that may be robust. Improving systems information for security nation must saddle contain mechanisms that reduce the impact of cognitive biases on process decision-making. by integrating a decision framework hybrid, developing some Explainable AI, application of anti-disinformation mechanisms, and placing multi-scenario simulations, security systems can become may robust and resistant to threats emerging. systems information modern incorporates patterns thinking humanity by using predictive models and intelligence algorithms, influencing thus the process of decision-making in security national. Although these systems can contribute to an analysis that may quick and efficient A threats, they are subject to risk-associated cognitive biases and lack of transparency. In the future, the integration of some AI audit mechanisms and the development of some models will be essential for ensuring making some decisions are balanced and correct. In addition, the advanced technological It could lead to increasingly complex systems may autonomous, which require regulation ethics to prevent abuse and to maintain the trust of the public in security institutions national. Perspective future suggests an evolution of significant systems information to autonomy and interconnectivity extended. Advances in learning automatically and in intelligence algorithms are artificial to allow the creation of some systems capable saddle advancing and preventing threats cyber and geopolitical with a high degree of precision. At the same time, the development of some standard ethics and regulations will become vital for the prevention use insider of these technologies. It is possible that, in the future, governments will implement mechanisms of international cooperation to ensure the use of AI is responsible for security national. In addition, the system's future will be saddle contain capabilities of advanced interpretation and adjusting decisions, reducing the risk of some bugs due to cognitive biases and improving transparency process decision-making.

References

Brown, K. W. & Green, J. D. (2022). The Role of Emotions in Decision-Making Processes. *Emotion Review*, 14(1), 45-58.

Dragomir, F. L. (2016a). Models of Trust and Reputation in eCommerce. *OEconomica*, 12(6), 235-242.

Dragomir, F. L. (2016b). Recommendation and reputation in eCommerce. *EuroEconomica*, 25(2), 151-155.

Dragomir, F. L., Dumitriu, C., & Bărbulescu, A. (2021). Recommendation Systems-Modeling Abusive Clauses in E-commerce. *International Conference on Electrical, Computers, Communications and Mechatronics Engineering*, IEEE, 1-4.

Evans, J. S. B. T. (2022). Dual-Process Theories of Decision-Making: A Selective Review. *Annual Review of Psychology*, 73, 511-534.

Garcia-Retamero, R. & Dhami, M. K. (2020). On the Psychology of Decision-Making under Uncertainty. *Psychological Review*, 127(5), 691-713.

Gigerenzer, G. & Gaissmaier, W. (2011). Heuristic Decision Making. *Annual Review of Psychology*, 62, 451-482.

Harren, V. A. (1979). A Model of Career Decision Making for College Students. *Journal of Vocational Behavior*, 14(2), 119-133.

Johnson, P. T. & White, M. P. (2023). Social Influences on Decision-Making: A Review. *Social Psychology Quarterly*, 86(1), 1-20.

Kahneman, D. & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, 47(2), 263-291.

Klein, G. (1993). *A Recognition-Primed Decision (RPD) Model of Rapid Decision Making. Decision Making in Action*. Ablex.

Lee, A. Y. & Schwarz, N. (2021). Risk Perception and Decision-Making: The Role of Affect. *Journal of Risk Research*, 24(5), 567-582.

Simon, H. A. (1995). A Behavioral Model of Rational Choice. *The Quarterly Journal of Economics*, 69(1), 99-118.

Smith, J. A. & Doe, R. L. (2021). Intuitive Decision-Making in Uncertain Environments. *Journal of Behavioral Decision Making*, 34(2), 123-135.

Tache, F. L. (2009). Advice in electronic commerce. *3rd International Workshop on Soft Computing Applications*, IEEE, 111-114.

Tache, F. L. (2010). Trust model for consumer protection (TMCP). *4th International Workshop on Soft Computing Applications*, IEEE, 107-112.

Tache, F. L., Postolache, F., Năchilă, C., Ivan, M. A. (2010). Consulting in electronic commerce. *OEconomica*, 6(3), 162-169.

Taylor, S. E. & Thompson, S. C. (2020). Adaptive Rational Decision Strategies. *Cognitive Psychology*, 115.